ISSN (Online) : 2454 -7190 ISSN (Print) 0973-8975
J.Mech.Cont.& Math. Sci., Vol.-13, No.-4, September-October (2018) Pages 73-89

Blockchain Based E-Stamp Procurement System with Efficient Consensus Mechanism and Fast Parallel Search

[1]Nikita Singh, [*2]Manu Vardhan

[1,2] Department of Computer Science and Engineering
National Institute of Technology Raipur
Great Eastern Rd, Amanaka, Raipur, Chhattisgarh 492001

E-mail: [1]nikitasinghk@gmail.com, [2*]mvardhan.cs@nitrr.ac.in

*Corresponding Author: Manu Vardhan

Mobile: (+91)8853038545, E-mail: mvardhan.cs@nitrr.ac.in

Abstract

Digital Ledger Technology (DLT) is fast growing as solution to various financial applications that require secure and temper proof transactions system. The blockchain based system is a decentralized system for storing the information in consistent and virtually centralized environment. This paper proposes blockchain based application for e-stamping facility along with new consensus algorithm and optimized search algorithm. To achieve consensus for the newly mined block, it is proposed that only trusted nodes are selected for voting. This reduces broadcasting overhead to multicasting to about 50% of nodes. The proposed fast parallel search algorithm reduces the overall search time by 1/5 as compared to the existing algorithms. This is done on a subset of block chain against complete blockchain. Finally, the system can be adopted for the digitalization of the e-stamp facility and process where the stamp duty is required. The government authorities can also authorize private organization for selling the e-stamp to generate the revenue. The system can be able to detect any fraudulent activity.

Keywords: Blockchain**,** Consensus Mechanism, Block Search, Trust, P2p

I. Introduction

Alm et al. [I] carried out a detailed study on the various options for reforms of stamp duties levied by different state governments on any transaction of immovable property in India. The authors examine and reviewed various government practices and the difficulties experienced in terms of taxation, mode of collection and its impact on economy. They also highlight the impact of higher taxation in terms of stamp duties that leads to under-declaration of the value of immovable property that paves way for transacting with black money. This aspect of under declaration can clearly be eliminated by the adoption of DLT by recording all the registries of immovable properties in blockchain. Authority can trace back all the transactions that have taken place on this immovable property. This shall allow them to trace the phenomenon of under declaration and thus prevent tax evasion. Digital Ledger

Technology (DLT) is fast growing as solution to various financial applications that require secure and temper proof transactions system. It consists of blockchain that not only fulfills all the requirement of any financial application but also provides decentralized management to them [XIII]. The very intrinsic nature of blockchain i.e. immutable records of transactions on distributed ledgers renders itself useful for use by various functionaries of Government. Government offices offer various public schemes and most of these involve finances. Hence, there is need for a system that is efficient, fast, fraud free, tamper proof and trust worthy. Most of these can be offset by moving to DLT.

A block is a data structure that aggregates or batches multiple transactions into a suitable size of structure. The series of immutable blocks form a blockchain. Each block header contains hash of previous block. The secure hash algorithm namely SHA256 [IV] is the backbone of the all the blockchain applications. The SHA256 generates unique and one way hash value. This property of secure hash algorithm creates immutable blocks in blockchain. The content of the block are immutable since any attempt to modify content of a block shall result in a different hash value of this block rendering it inconsistent and discoverable. This is because; hash of this block is recorded in header of successor block. In order to change any content of a single block in the middle of a blockchain, all subsequent blocks need to be changed. Since all peers has replica of this blockchain, this is impossible to achieve. Hence it is robust and immutable. Thus, it is an append-only sequential data structure. A blockchain is unsuited for data manipulation, being designed for the very specific idiosyncratic task of immutability. The blockchains are subset of distributed ledgers. Each block also has digital signatures generated by RSA cryptographic [XVII] keys. The Elliptic Curve Digital Signature Algorithm (ECDSA) [VIII] is widely used in blockchain application. The Signature generated by the private key using ECDSA can be verified using the corresponding public key. To achieve the decentralized system, all blockchain application uses p2p network. This p2p network forms a overlay network over the underlay TCP/IP network [XXII].

II. Related Work

DLT is an upcoming area which is still in its nascent form. Many of the challenges are still in the conceptual form with many researchers and companies working on it. Guo and Liang [VI] propose complete decentralization in the operation of banks and promote use of blockchain based methods in order to reduce the time of reconciliation. Moreover, many nations have still not come up with the regulatory frameworks in order to regulate blockchain based solutions. They also propose regulatory sandbox where the implementer or the bank has sufficient space for innovations without regulatory hurdles. They also stress on the need for stricter access mechanisms for the blockchain based banking applications.

Sward et al. carried out a comprehensive survey of the benefits and drawbacks of various data insertion methods in block chain [XX]. They reveal that there exists no optimal data insertion method that outscores all the existing mechanisms. It is proposed that the data insertion method is a function of the application being built, amount of data and various priorities. Batubara et al. discuss about various challenges while building applications using block chain [II]. This includes technological aspects such as flexibility, scalability and security. In terms of issues that have to be considered by any organization wishing to move to blockchain, issues of acceptability and governance models have been discussed. Legal and regulatory aspects also pose challenges. Hou [VII] discussed various applications of the blockchain that can be use in e-governance model. In these applications, the digital information sharing and digital credit sharing are based on the blockchain model are discussed. Nguyen [XVI] discussed the role of the blockchain in secure and sustainable development in the financial system. The article shows that it right time to adopt the blockchain technology on all the financial applications. Mettler [XII] proposes various application of the blockchain in healthcare. The blockchain based application can be used for maintaining patient records, drug information etc.

Transfer of immovable property in India is a tedious process that involves too many people and requires a tiring attention to detail that can discourage even the most optimistic people [XIX]. Counterfeit stamp papers leads to evasion of tax and the danger of any transaction being declared by the authorities looms over the buyer or the seller. If it is done by the seller, then obviously buyer looses out everything. In order to curb this, Government of India introduced e-stamping facility. The e-stamps are being sold only by Stock Holding Corporation of India Limited (SHCIL) using a centralized web interface. The only but major drawback of this arrangement is that the whole system is centralized. Verification of the details of previous property transaction can be very tedious affair. Also, the taxation authorities have no power to peek into the system and it remains on the mercy of the registrar office for communication of transactions, which is often delayed. Also, very few banks and payment method are available for payment for procuring e-stamping.

When there are thousands of nodes that are part of p2p network, it becomes a tedious operation to invite votes from all the nodes while achieving consensus. Various consensus mechanism such as proof-of-work (PoW) [XV], Proof-of-stack (PoS) [IX], proof-of-elapsed time [V] are used in various blockchain based application. Trustworthy miner selection is also the responsibility of consensus algorithm. Vardhan and Kushwaha [XXI] propose trustworthiness of nodes for maintain file consistency in cluster environment.

All these challenges can be offset if the system of procurement is moved to blockchain or also referred as Digital Ledger Technology (DLT). The system is decentralized and can be integrated nationwide, which today is state wide. Payment can be made online through net banking or e-wallet. Tax authorities can be provided a web interface in order to keep an eagle eye on various transactions. It shall be very easy to discover high value transactions and frequency of transactions being carried out by an individual or a company. This also demands efficient search strategy and consensus mechanism. This research proposes a solution for these issues.

III. Proposed Work

This paper proposes a secure and decentralized system for sale of e-stamp that is based on the blockchain and p2p network. In the p2p network as proposed in figure 1, the existing authorized agency for selling e-stamp i.e. Stock Holding Corporation of India (SHCI) shall be required to set up some miner nodes in various regional offices. These miner nodes will store e-stamps details in the blockchain and local repository. The p2p network involves all the miner nodes and the nodes established by various government organizations that use e-stamp for different activities and transactions. These nodes are vested with the job of verifying the originality of the e-stamp by searching its details in blocks in the blockchain. In the proposed system, each miner node has to provide a web application to the public domain for e-stamping facility. This web-application is connected with the blockchain via the interface provided by the miner and regional offices. This web application provides a facility to public for purchasing of e-stamp. The complete system is decentralized hence not vulnerable to single point of failure. The architecture of proposed system is shown in the figure 1.

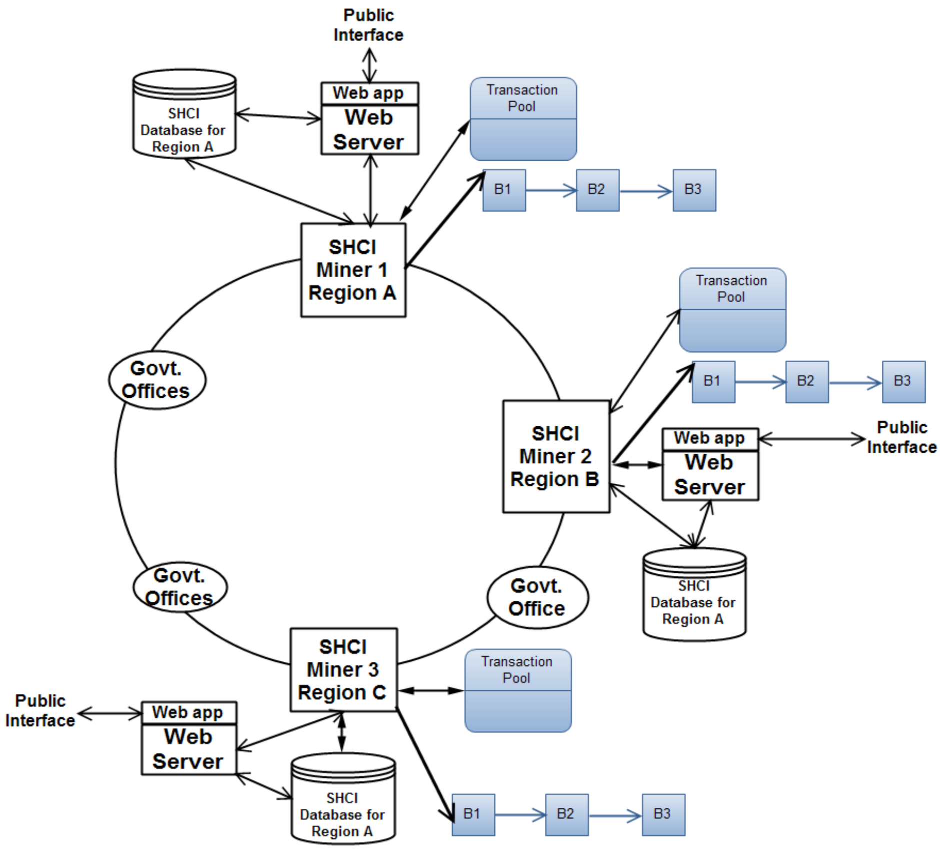

Figure 1. Network architecture of proposed e-stamping system

The network uses Interplanetary File System (IPFS) [XXII]to form the p2p swarm. Any authorized node that can either be miner or non miner can join the network with the help of bootstrap server. The bootstrap server must be under control of the centralized authority which in this proposal happens to be SHCI. This bootstrap server does not play any role in functioning of blockchain. It just maintains the list of active and inactive nodes in the network. To join the network any authorized node can get list of other active peers from bootstrap server and connects with those peers individually. Each miner node only stores all the details of e-stamps issued by miner itself in a local database. All other organizations that are willing to accept the e-stamp shall set up IPFS nodes. These nodes can join the swarm network and verify the authenticity of e-stamp by searching in the blockchain. The proposed works involves mainly following two modules namely:

- Generating the E-Stamp and Block generation
- Verification of E-stamp

These three activities are described in the succeeding section.

III.a. Generating the E-stamp

Any end-user / buyer that need e-stamp shall use the web interface provided by regional offices/miners. User has to fill all the necessary details to obtain the e-stamp. The web interface collects these details and generates corresponding request for e-stamp generation. The end-user is required to pay the required stamp duty via the e-wallet interface provides by banking system. Each miner node also has e e-wallet account in the banking system. After the successful transaction of stamp duty by the end-user to the corresponding e-wallet account, miner node gets acknowledgement from its e-wallet interface and approves the request. Each of these steps is illustrated in figure 2.

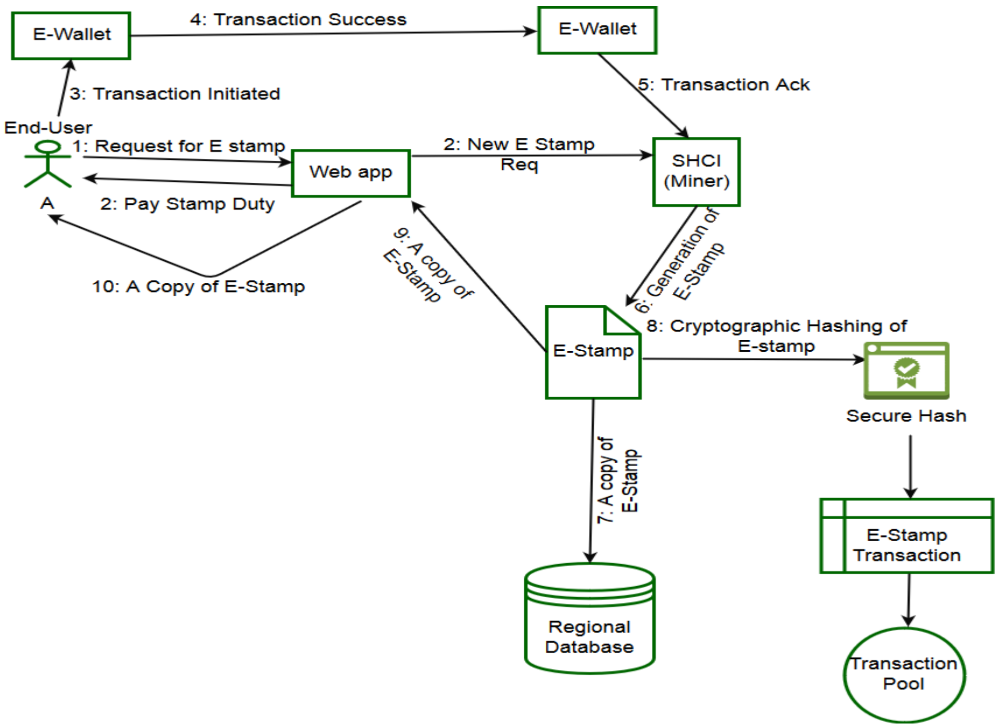

Figure 2. Collaboration diagram for e-stamp procurement

Miner generates an e-stamp and attaches the digital signature of the signing authority. Therefore, in the proposed system, each miner must have a signing authority. This authority has RSA cryptographic key pair of public and private key. The public key of the each authority is known to all other nodes while private key is kept secret to the authority itself. Each transaction related to e-stamp is signed by signing authority using its digital signature generated by private key. Other nodes can verify authenticity of digital signature signed of any authority by using public key of the corresponding authority. The generated e-stamp also has a unique barcode. This barcode number can retrieve the associated e-stamp details. The e-stamp generated by miner is stored on local database along with necessary detail; a copy of the e-stamp is placed in transaction pool in the form of one individual transaction. Five such transactions are placed in one block. At last a copy of the e-stamp is delivered to the end-user via web interface.

Collection of stamp duty using e-wallet facility

Purchasing e-stamp requires payment of stamp duty by the users. The proposed system provides a web interface for payment of the stamp duty through a payment gateway. Banking systems are exploring means and ways to adopt e-wallet facilities for their users. Various banks in India are also trying to develop blockchain based interoperable e-wallet system. Singh et al. [XVIII] propose a novel framework for interoperable e-wallet system for banking transactions. This proposed system also provides the payment of stamp duty via e-wallet system. To provide this facility, all the regional offices that are also miner in the proposed blockchain have to maintain e-wallet facility from any participant bank. So any transaction through e-wallet facility is also reflected in the proposed system. The miner nodes have to maintain e-wallet application and e-stamp blockchain. The transfer of amount through e-wallet application is illustrated in fig 3. It shows that User A transfers some amount using e-wallet facility to the miner's account from where he procures e-stamp. In this facility, public key of miner is playing the role of beneficiary address.

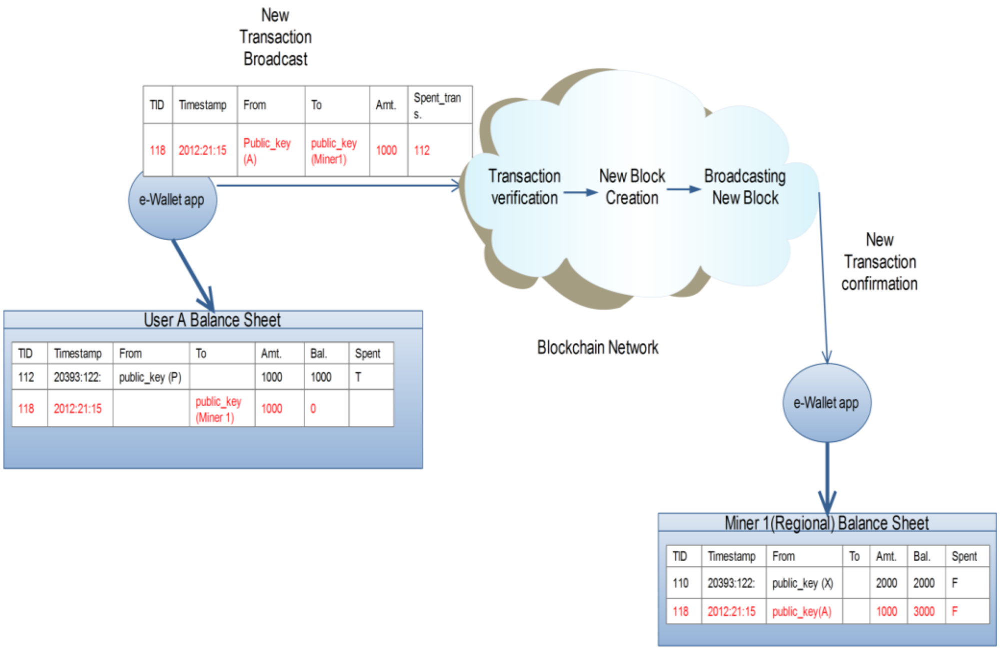

Figure 3. Illustrating transfer of stamp duty between User's wallet to regional office's wallet

The miner nodes have to store all these e-stamp transactions into the blockchain. The miner has to prepare a transaction for each issued e-stamp. This transaction contains attributes such as certificate number, barcode number, state name, duty type, date of issue, duty amount, buyers name, buyer's identity card number, buyers address. The transaction is comprised of all these attributes and SHA256 hash value of all attributes. Generation of an individual e-stamp transaction is mathematically explained as under:

Let the attribute of the transactions be defined as a set A_t, such that

$$A_t = \{C_N, B_N, State_{Name}, D_T, I_D, D_A, BY_N, BY_I, BY_{ADD}\}$$

where,

C_N is the Unique certificate number,

B_N is the unique bar-code number,

$State_{Name}$ is the name of state for which buyer purchasing the stamp,

D_T is the type of duty stamp,

I_D is the stamp issued date,

D_A is the duty charge on the stamp,

BY_N is the name of buyer,

BY_I is the identity card number of the buyer,

BY_{ADD} is the address of the buyer,

The secure hash of the attribute set is defined as:

$$Hash_{A_t} = SHA256\,(A_t) \tag{1}$$

Here, SHA256 will return secure hash value of the input argument.

Let, public and private key of the signing authority be P_K and S_K respectively. Hence, the digital signature generated by Elliptic Curve Digital Signature Algorithm (ECDSA) is defined as:

$$DS = ECDSA\,(S_K, SHA256\,(Hash_{A_t}, A_t)) \tag{2}$$

$$T_X = \{A_t, Hash_{A_t}, DS\} \tag{3}$$

An e-stamp transaction (T_X) can be defined as set of attribute set, hash of attribute and digital signature of signature authority. This is represented as:
The authenticity of the generated Digital Signature (DS) is verified by ECDSA_PR proof checking function by passing DS and public key P_K in this function. Hence, Authenticity of digital signature be defined as:

$$V = ECDSA\_Pr(DS, P_K) \tag{4}$$

If the value of V is true, then the digital signature is said to be valid otherwise the signature is invalid. In the proposed system, each miner nodes have public key of all the authority.
Once a transaction is verified, then five such transactions are placed in a block as illustrated in figure 4. The secure hash value of all the attributes makes transaction immutable. All miner nodes in the network go through the same process for e-stamp generation. A block is defined as collection of the transaction sets along with the hash of previous block and the signature of the verifier.
Hence,

$$Block = \{Pre_{Hash}, T_{X_1}, T_{X_2}, ...T_{X_5}, DS\} \tag{5}$$

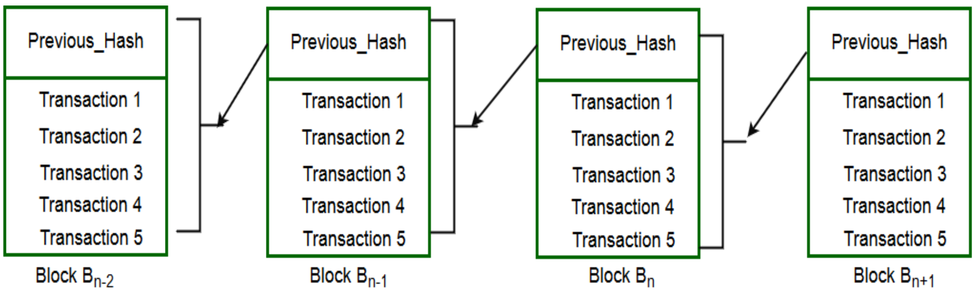

Figure 4. Blockchain structure of proposed system

Since all the regional nodes are responsible for generation of the digital registry documents, hence each regional node requires capability of mining the blocks. This demands leader election and consensus mechanism in order to establish correctness of these transactions stored in these blocks. In order to provide equal opportunity to each node, this paper proposes fair leader election approach along with a novel consensus algorithm.

Leader Election & Consensus Algorithm

The proposed blockchain system consists of the nodes that are part of the registry office spread throughout the states, termed here as Official Miners (OM). In this approach, each regional node will get fixed time slot for creation of the new block and all other nodes must wait for their turn to get their slot. It also consists of Private Miners (PM). The private miners are entrusted with the task of mining operation. These miners get the incentive for block / transaction verification. Since, there shall be thousands of registry offices; it is not feasible that all these nodes participate in consensus process. This shall slow down the system considerably and incur huge computation and bandwidth overhead.

We compute the Trust Value (TV) [XIV] of all these nodes based on the following two parameters:

i) Computation Power and Response Time (CPRT) of each node along with its communication (bandwidth) time &

ii) Trustworthiness based on history of Correctness of Transaction (CoT) verification during any new block addition process.

If CPRT is <30 Sec, its TV is incremented by 2. If it lies between 30 & 60 sec, it is incremented by 1 else by 0.5. Similarly, for every correct verification done by a miner, CPRT is incremented by 1 else decremented by 5. This is because there is no scope for malicious / incorrect transaction.

Based on these TV, following three groups of nodes is identified:

G1: Highly reliable Official Miners,

G2: Highly reliable Private Miners &

G3: Moderately reliable OMs & PMs.

When a new block is created, it is broadcast to all OMs & PMs. For attaining consensus, only 50% of G1 & G2 nodes are selected and 30% nodes from G3 are selected. So it is multicast to fewer nodes as compared to broadcast done by existing systems. Based on the outcome of this verification process, if majority vote is achieved, all the nodes are intimated and the new block becomes part of blockchain. So this proposed method reduces the overhead of broadcasting a new block reduces by more than 50%. This again saves computation time and network bandwidth.

III.b. Verification of E-stamp

E-stamp issued by any miner is legal and valid to be used in any region. These e-stamp details are stored in the blockchain. Any organization that accepts e-stamp can join the proposed p2p network or can use the proposed web application in order to verify the originality of the e-stamp as illustrated in figure 5. To verify the e-stamp, any node can broadcast the verification query by using the barcode printed on the e-stamp. The other nodes search the requested barcode in the blockchain. After the verification of the e-stamp, all participating nodes send their votes to the requester node as explained in consensus mechanism. The requester node can approve the validity of the e-stamp based on the majority of the votes. The verification process can't be tampered and any fraudulent node can't validate fake e-stamp.

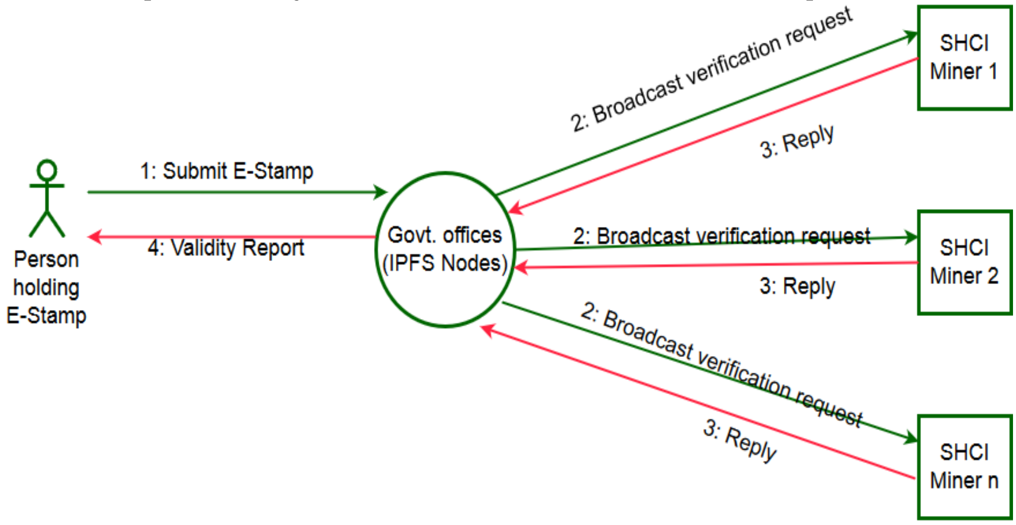

Figure 5. E-stamp Verification Process

All the above discussed operations demand scanning and searching for details of one e-stamp among millions of blocks that are part of a single nationwide blockchain. Sequential search shall be highly time intensive with poor response time. Hence an efficient search mechanism is proposed in the next section.

Fast Parallel Search Algorithm

Transactions are held in block. We propose JavaScript Object notation (JSON) [III] file format for recording transactions into a block. This facilitates efficient search based on key value pair. Whenever a registry has to take place, the blockchain is accessed in order to fetch the block that contains the seller details. It also has to verify e-stamp. This requires multiple block traversals. When the blockchain grows bigger, it may warrant back traversal of millions of blocks. This process is CPU time intensive. We propose a parallel search algorithm in order to reduce this time considerably. In the proposed algorithm, each miner maintains metadata about the blockchain in separate table. In metadata, the hash of the intermediate blocks will be saved in fixed date interval as shown in table 1. It is expected that about 5 million transactions take place in a month for procurement of e-stamp. The metadata table stores hash of the last block added to the blockchain for each month. This can be reduced to either fortnightly or bimonthly depending on the volume of blocks being generated. This strategy drastically reduces the search space.

Table 1: Blockchain Metadata Table

S. No.	Date		Date Interval	Hash of the Intermediate Block
	From	To		
1	01-01-2018	31-01- 2018	31 Days	QmfAGjNzbpdwXMxCTMQf4Pu3ptGoax5qb3tXjNBxgAVq
2	01-02-2018	28-02-2018	28 Days	QmP89381CtKqLUCS6a3sPEnnvLEdKMstFgyCAhpo5RHutX
3	03-03-2018	31-03-2018	31 Days	QmPzXufcGZ75VppABfFTpHffctgiAyfQQJs1xzTwh1Lxdokl
....	....	....	....	....

The constituents of table 1 are illustrated in figure 6.

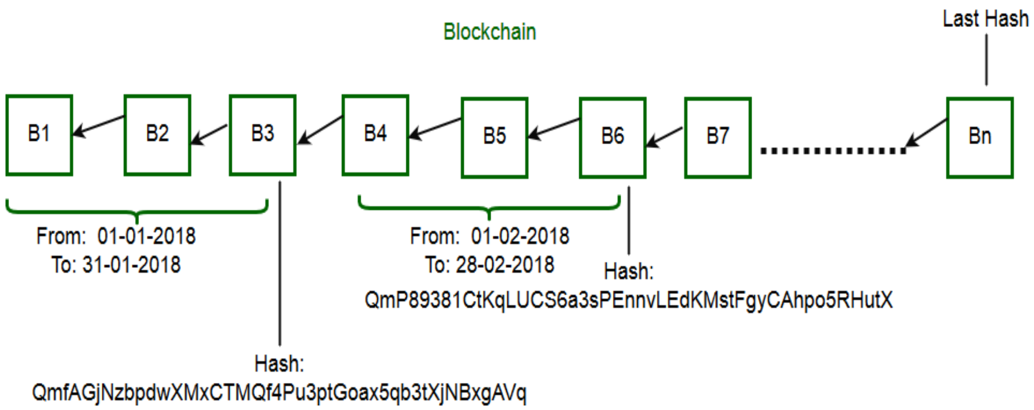

Figure 6. Representation of the sub-blockchain for fast parallel search algorithm

When any e-stamp is submitted for any job, it is first verified by the miners. The miners extract the date of issue of e-stamp and finds the hash of the block from metadata where the block is to be searched for. This is nothing but a sub blockchain. Thus, metadata information can be used to find the hash of the block that contains the requested stamp. During the verification process, miner extracts the hash of the intermediate blocks in blockchain and starts search from intermediate block instead of the last block of the blockchain. If it is a verification request for the e-stamp issued on 08-02-2018, search algorithm selects the sub-blockchain based on the date interval and start searching for each block for particular e-stamp as shown in the figure 6. Now to search the particular transaction from the block, we propose to reduce the search time by introducing thread level parallelism. Since there exist five transactions per block, the search algorithm searches with six thread process.

First five threads read each transaction in order to search a transaction record. The sixth thread points to the preceding block as illustrated in figure 7. The thread that finds the desired transaction record sends message to all such processes and the search stops. The time saved is again reduced by 1/5 for each block.

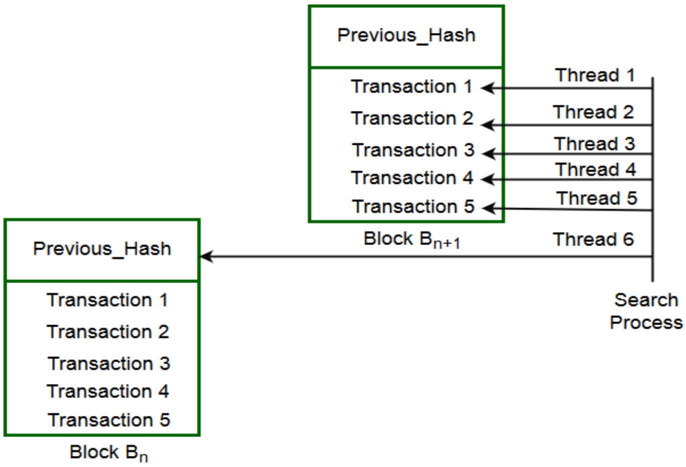

Figure 7. Parallel Searching in Proposed System

IV. Implementation & Results

Implementation of the proposed approach requires creation of the p2p network, development of the blockchain application and the web application. In this proposed approach, p2p network is created using the IPFS utility. The necessary bootstrap program for the proposed application is developed in the 'C' programming language. This bootstrap server program provides list of the all IPFS nodes in the network through the bootstrap client program. The application to maintain the blockchain is developed in Java programming language using IPFS utility. A web application is also developed in JSP to provide the public interface for e-stamp purchasing. Figure 8 shows the application stack for the IPFS node for miner.

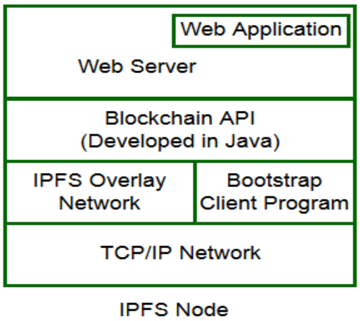

Figure 8. Application Stack of Miner (IPFS Node)

All the miner nodes in the networks communicate through the blockchain API that built upon the IPFS network. The web application has only limited access to the core of the IPFS network. Blockchain API provides the interface for web application. The complete blockchain is stored in the IPFS network. In order to illustrate the functioning of the proposed system, a case study is performed wherein the proposed e-stamping system is integrated with e-property registration system. The effectiveness of the proposed system is measured in terms of the number of interactions required for end user to buy a property.

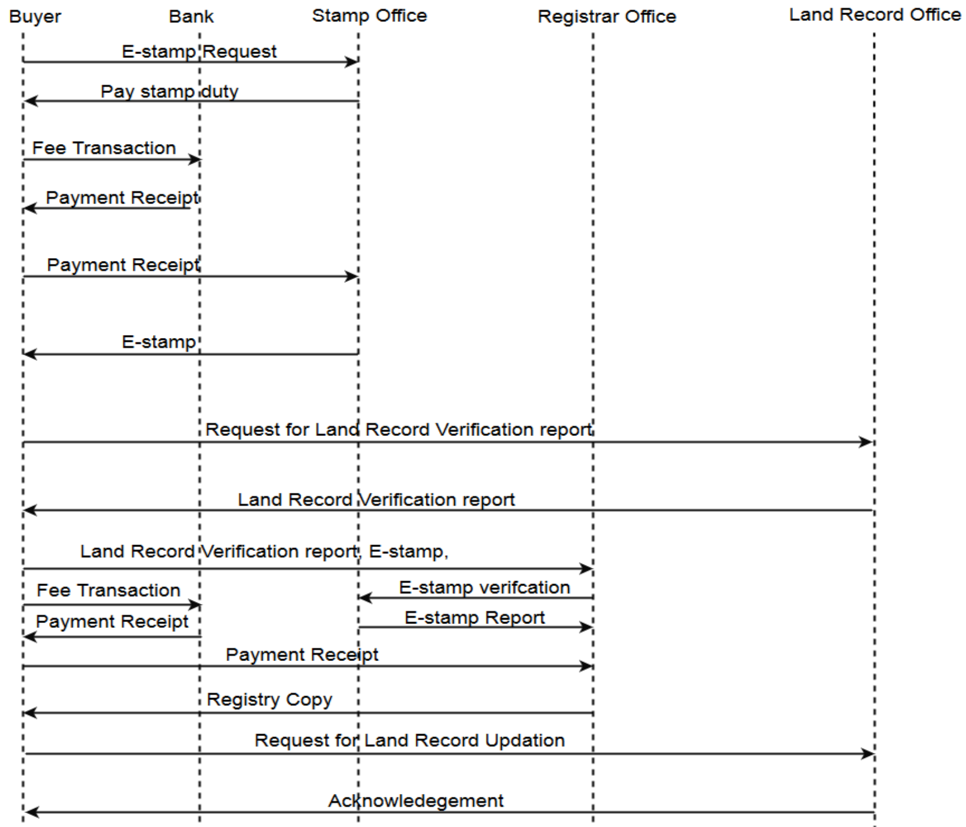

Figure 9. Interaction required for Buyer/End-user to purchase a property in existing system

Figure 9 shows the number of interaction that happens in general property transaction with existing manual system. The existing system requires at least 15 interaction of message between buyer and the various offices. This system is based on manual verification and manual registry process. In the proposed system as illustrated in figure 10, all government offices can join the blockchain and the verification of e-stamp can be done using proposed DLT based verification system and registry of the property can also be generated and stored using blockchain. All verification interactions happen internally. The buyer/end-user need to interact with 50% less number of message. The approach also becomes automatic and distributed in nature.

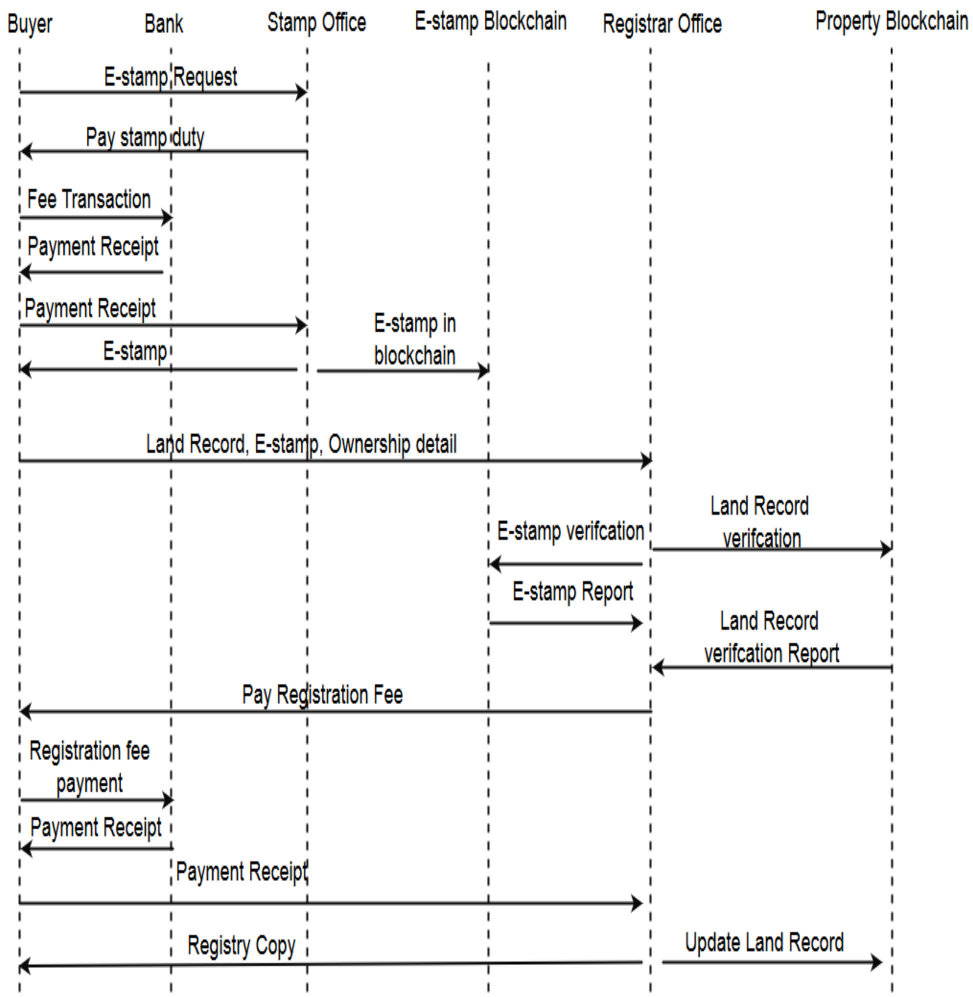

Figure 10. Interaction required for Buyer/End-user to purchase a property in proposed system

The proposed system is a decentralized system but the information in the system is kept in a virtually centralized way. The information is consistent as well. Table 2 shows the comparative features of the proposed system with the existing system.

Table 2. Comparison of Proposed System with existing system

S. No.	Features	Existing System	Proposed System
1	E-stamp purchasing interface for public domain	Single interface only	Multiple interface only
2	E-stamp verification interface for public and authorized domain	Single interface for both domains	Multiple and different interface for public and authorized domains
3	Centralized repository of the documents	Only E-stamp records are centralized	The complete system is decentralized but information is virtually centralized
4	Digitalization of documents	Not possible	Complete digitalization of documents is possible due to DLT
5	Security of documents	Not so secure, digital e-stamp can be tempered and verification process can be hacked	Completely secured due to cryptographic hash and decentralized system. Hacking and alteration of blockchain hasn't been reported till date.
6.	Ease of uses	More difficult due to number of interaction required by end-user with different departments.	Easy for public domain due to all major interaction being internal are automatic.

V. Conclusion

This paper proposes a novel system for e-stamp selling. This system is based on the concept of blockchain technology wherein the records are stored in the immutable block. The blockchain proposed in this paper is permissioned blockchain hence only authorized nodes can join the network. The web interface of the proposed system connects the public to the system with restricted roles. The proposed system reduces the number of interaction for property registration by 50%. A novel and efficient consensus mechanism is also proposed since it is DLT based. To achieve consensus for the newly mined block, it is proposed that only trusted nodes are selected for voting. This reduces broadcasting overhead to multicasting to about 50% of nodes. Existing blockchain based systems require traversing the blockchain in order to search for the required block. This paper proposes fast parallel search algorithm for optimized search mechanism. The proposed search algorithm searches the blocks by generating parallel threads for comparing the transactions that reduces the overall search time to 1/5 times as compared to the existing algorithms. This is done on a subset of block chain against complete blockchain. Finally, the system can be adopted for the digitalization of the e-stamp facility and process where the stamp duty is required. The government authorities can also authorized private organization for selling the e-stamp to generate the revenue. The system can be able to detect any fraudulent activity.

References

I. Alm, J., Annez, P., Modi, A.,"Stamp duties in Indian states: a case for reform". The World Bank (2004).

II. Batubara, F.R., Ubacht, J., Janssen, M., "Challenges of blockchain technology adoption for e-government: a systematic literature review". In: Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. p. 76 (2018).

III. Crockford, D., "The application/json media type for javascript object notation (json)". (2006).

IV. Eastlake 3rd, D., Jones, P., "US secure hash algorithm 1 (SHA1)". (2001).

V. Ferrer E.C., “The blockchain: a new framework for robotic swarm systems,” arXiv Prepr. arXiv1608.00695, 2016.

VI. Guo, Y., Liang, C., "Blockchain application and outlook in the banking industry". Financial Innovation 2, 24 (2016).

VII. Hou H.,"The application of blockchain technology in E-government in China". In Computer Communication and Networks (ICCCN), 2017 26th International Conference on 2017 Jul 31 (pp. 1-4). IEEE.

VIII. Johnson, D., Menezes, A., Vanstone, S., "The elliptic curve digital signature algorithm (ECDSA)". Int. J. Inf. Secur. 1, 36–63 (2001).

IX. King S. and Nadal S. “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,” self-published Pap. August, vol. 19, 2012

X. Kumari, A., Mishra, S., Kushwaha, D.S., "A New Collaborative Trust Enhanced Security Model for Distributed System". Int. J. Comput. Appl. 1, 127–134 (2010).

XI. Lua, E.K., Crowcroft, J., Pias, M., Sharma, R., Lim, S., "A survey and comparison of peer-to-peer overlay network schemes". IEEE Commun. Surv. Tutorials. 7, 72–93 (2005).

XII. Mettler M., "Blockchain technology in healthcare,The revolution starts here". Ine-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on 2016 Sep 14 (pp. 1-3). IEEE.

XIII. Mills, D.C., Wang, K., Malone, B., Ravi, A., Marquardt, J., Badev, A.I., Brezinski, T., Fahy, L., Liao, K., Kargenian, V., others, "Distributed ledger technology in payments, clearing, and settlement". (2016) Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2016.095., .

XIV. Mishra, S., Kushwaha, D.S., Misra, A.K.: Jingle-Mingle, "A Hybrid Reliable Load Balancing Approach for a Trusted Distributed Environment". In: INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on. pp. 117–122 (2009).

XV. Nakamoto S., "Bitcoin: A peer-to-peer electronic cash system," 2008.

XVI. Nguyen QK, "Blockchain-a financial technology for future sustainable development". In Green Technology and Sustainable Development (GTSD), International Conference on 2016 Nov 24 (pp. 51-54). IEEE.

XVII. Shand, M., Vuillemin, J., "Fast implementations of RSA cryptography". In: Computer Arithmetic, 1993. Proceedings., 11th Symposium on. pp. 252–259 (1993).

XVIII. Singh K., Singh N. and Kushwaha D. S., "An Interoperable and Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain". In: Proceedings of the International Conference on Computing, Power and Communication Technologies 2018 (GUCON) (2018).

XIX. Shoaib Zaman, "Duly Stamped", Article in Money Today, Print Edition: January 2014, https://www.businesstoday.in/moneytoday/financial-planning/electronic-stamping-is-a-convenient-way-to-pay-stamp-duty/story/201780.html, Accessed on 16.08.2018

XX. Sward, A., Vecna, I., Stonedahl, F., "Data Insertion in Bitcoin's Blockchain". Ledger. 3, (2018).

XXI. Vardhan M, Kushwaha DS, "File replication and consistency maintenance mechanism in a trusted distributed environment". CSI Transactions on ICT. 2013 Mar 1;1(1):29-49.

XXII. Weblink for IPFS, https://ipfs.io/.